



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/500,955

09/03/2004

Alexander Shipp

117-515

1428

23117 7590 10/19/2007  
NIXON & VANDERHYE, PC  
901 NORTH GLEBE ROAD, 11TH FLOOR  
ARLINGTON, VA 22203

EXAMINER

NALVEN, ANDREW L

ART UNIT

PAPER NUMBER

2134

MAIL DATE

DELIVERY MODE

10/19/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

MN

<b>Office Action Summary</b>	<b>Application No.</b> 10/500,955	<b>Applicant(s)</b> SHIPP, ALEXANDER	
	<b>Examiner</b> Andrew L. Nalven	<b>Art Unit</b> 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 9/7/2007.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 15-26 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed:
- 6) ☒ Claim(s) 15-26 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 08 July 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>7/8/04</u> . | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

1. Claims 15-26 are pending.

### ***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. **Claims 21-26 are rejected under 35 U.S.C. 101** because the claims are directed towards nonstatutory subject matter. The cited claims are an example of functional descriptive material consisting of data structures and programs that impart functionality when employed as executed by a computer component. The functionality of functional descriptive material is realized only when the functional descriptive material is claimed as being embodied on a computer readable medium and is claimed as executed by a computer component. Examiner is unable to ascertain what hardware elements provides tangible computer components that work in conjunction with the functional descriptive material to impart functionality. Thus, the claims are not statutory because they fail the practical application requirement of § 101 by failing to provide a useful, concrete, and tangible result (see MPEP 2106).

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. **Claims 15-26 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Nachenberg US Patent No. 6,971,019 in view of Kephart et al US Patent No. 5,675,711.

4. **With regards to claims 15, 18, 21, 24,** Nachenberg teaches A method of detecting virus infection of an executable image (Nachenberg, column 9 lines 33-46, examines code at entry points to determine if infected by virus), the method comprising: determining the file type and the entry point of the executable image (Nachenberg, column 9 lines 33-46, examines code at entry points to determine if infected by virus, column 9 lines 33-46, examines code at entry points to determine if infected by virus); scanning the executable image, for start-up code at a location other than said entry point generated by one of the compilers used to generate the determined file type (Nachenberg, column 9 lines 33-46, identifies the main entry point of the program, column 5 lines 25-55, look for entry point for a particular file, example includes .exe, .dll, Apple files, column 5 lines 9-25, JMP or CALL modified to jump to a viral code, column 7 lines 10-21, modified instruction becomes new entry point, column 9 lines 40-46, look for suspicious JMP or CALL); and flagging the executable image as suspicious from the point of view of possibly containing a virus infection in response to it being determined during the scanning that the executable image contains said start-up code at a location other than said entry point (Nachenberg, column 9 lines 33-46, examines code at entry

points to determine if infected by virus). Nachenberg fails to teach identifying by reference to a database of known executable image layouts, the layout to which the executable image conforms. However, Kephart teaches teach identifying by reference to a database of known executable image layouts, the layout to which the executable image conforms (Kephart, column 4 lines 55-63, determining the compiler that was used to generate a particular program). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Kephart's method of compiler identification because it offers the advantage of allowing reverse engineering of code to further the analyzing of computer viruses (Kephart, column 2 lines 1-15).

5. **With regards to claims 16, 19, 22, 25**, Nachenberg as modified teaches the database of start up code characteristics includes records of data values associated with routines which form part of the start up code (Kephart, column 4 lines 55-63, determining the compiler that was used to generate a particular program, column 5 lines 15-30, looks for patterns of data strings that match expected occurrences) and the step of scanning the executable image corresponding to at least one such data value and comparing it with that value (Nachenberg, column 9 lines 33-46, examines code at entry points to determine if infected by virus, Kephart, column 5 lines 15-25, identifies features present that are relevant to the classification decision, looks to the defined feature set).

6. **With regards to claims 17, 20, 23, 26**, Nachenberg teaches performing remedial action in respect of executable images flagged as suspicious from the point of

view of possibly containing a virus infection (Nachenberg, column 3 lines 40-45, reports virus being detected).

### ***Conclusion***

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.
8. Nachenberg US Patent No. 6,357,008 discloses a dynamic heuristic method for detecting computer viruses using decryption exploration and evaluation phases.
9. Arnold et al US Patent No. 5,440,723 discloses a system for automatic immunity for computers and computer networks.
10. Kephart et al US Patent No. 6,016,546 discloses a system for efficient detection of computer viruses and other data traits.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Andrew Naiven

A handwritten signature in black ink, appearing to read 'AN', is written over a horizontal line.